Wireless Safeguards for End Users and
Safeguards for Network Administrators and ISOs

Recommended by the California State ISO Office
July 2005

Safeguards for End Users

Below are some suggested safeguards for the users of wireless technology. The three main end-user risks associated with wireless technology are

- the possibility of sensitive or confidential information being transmitted without encryption, through which it could be made available to others,
- accidental or careless file sharing over the wireless network, allowing access to sensitive or confidential information stored on the wireless device, and
- unauthorized access to State networks.

As a portable computer user, you may be able to access wireless networks (WLANs) when you are away from your office even though your office does not have a WLAN. Some types of access involve authorized connections with a WLAN in a hotel, airport, or coffee house. There is usually a charge for this, but some businesses provide free wireless access as a customer service. While it is sometimes possible to gain unauthorized access to a WLAN, this is not a legitimate use of state resources and can be risky.

It is important to configure mobile devices properly and to be aware of the risks and the appropriate safeguards. Here are some precautions to help you use wireless laptop and handheld computing devices safely.

Avoid accidental or unsafe transmissions:

1. Disable the wireless interface when it is not needed. This can be done easily by using the wireless icon at the bottom of the screen; the interface can be reactivated easily when and if its functionality is needed.

2. Do not connect to anything identified as an "Unsecured wireless network" on the Available Wireless Network list that appears when the wireless interface is enabled. If your wireless device connects to an unsecured network, data will not be encrypted during transmission unless you are correctly using Virtual Private Network (VPN) software; exposure includes passwords and any sensitive or personal information.

3. If you have VPN software on your device, make sure that it is configured appropriately for traveling (ask your technical support staff for help if needed), and use it to encrypt your internet sessions.

Protect your files from being accessed by unauthorized parties:

1. Don't turn on the file share option unless it is absolutely needed and approved by your ISO. If it is already turned on, you should turn it off to make sure that outsiders do not gain access to your work or personal files. If you need to share some files for approved business purposes, don't share the entire hard drive;

share only specific folders and use strong passwords. Ask your IT support staff for help with this if needed.

2. Leave the personal firewall turned on. This comes with your operating system on Windows-based equipment and should already be turned on when the equipment is delivered; there is no reason to disable it. If it is not already turned on, you should do so before using the wireless capabilities of your laptop or notebook. Your IT staff should be able to help you do this if needed.

3. Disable the wireless function before connecting to a State network through a hard-wired docking station. (Many portable computer users also use docking bays in their offices to connect to their Department networks. Allowing the wireless device to continue to function while physically connected to a Department network could expose the workstation and the rest of the network to a hacking technique known as War Driving.) Either remove the wireless access card from the computer, or disable the wireless function when you are signing on to your non-wireless network.

Observe general end user wireless safeguards:

1. Keep all operating system software (Windows, for example) and key software patches up to date. Ask your department's IT staff for help with this if you are not sure how to do it.

2. Keep all anti-virus definition files and software up to date. Ask your IT staff for help with this if you are not sure how to do it. Make sure that you do your updates even when you are out of the office.

3. Don't install unauthorized wireless access points (APs) in your office. The only APs in your office should be those installed by and supported by your department's IT staff.

4. Safeguard and physically protect your mobile device (laptop or notebook) and passwords.

Safeguards for Wireless Network Administrators and ISOs

Two major risks for wireless networks in offices and homes are

- the possibility of unauthorized users connecting to the networks and gaining inappropriate access to state or personal information, and
- attacks from outsiders, including the introduction of spyware or malware into the network.

Some department network administrators deploy and manage department WLANs. These are created by installing wireless APs or routers. Even if your office has only one AP, this will still create a wireless environment and could introduce new risks. It is important to set up the APs appropriately and to create appropriate policies and processes to protect your infrastructure and your department's information. Here are some safeguards to apply when setting up and managing WLANS

Prevent unauthorized access and discourage attacks

Practice Effective AP Configuration:

1. When deploying APs, limit the physical coverage area (for example, place APs near the center of the building instead of near outside walls) to reduce the risk of outsider access.

2. Turn off APs during non-business hours.

3. Do not allow your APs to broadcast the service set identifier (SSID).

4. Change default AP administrator password and Internet Protocol (IP) addressing scheme; configure the AP administration function so that it cannot be modified through a wireless interface.

5. Disable Dynamic Host Configuration Protocol (DHCP), and manually assign IP addresses to your end user devices.

6. Configure your APs to accept only recognized media access control (MAC) address connections. (Each wireless card has a unique MAC address. You only want to connect with the ones you know.)

7. Use the strongest available Wired Equivalent Privacy (WEP) key.

8. Use Virtual Private Network (VPN) with Triple Data Encryption Standard (3DES) encryption for the transmission of sensitive or confidential data; set up user equipment to use this technology appropriately. Train your users about how to use VPN while traveling.

9. Don't allow users to install unauthorized (rogue) APs in the office. Scan your site periodically for unauthorized APs, which can introduce the risk of intrusions.

Practice Effective Configuration and Educate Users:

1. For users that will not need the wireless functions on their laptops and handheld devices, disable this feature.
2.
3. Develop and publicize policies and processes for wireless. This includes hardening, strong passwords, patch management, periodic scanning for unauthorized APs, user responsibility for mobile equipment, and other safeguards to protect your environment.

4. Train your users.